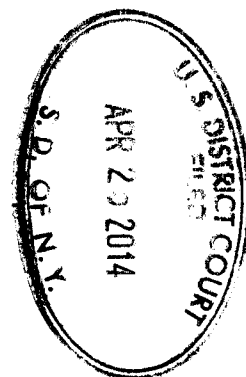


DOC # 98

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Search of The PREMISES
known and described as the email account
[REDACTED]@MSN.COM, which is
controlled by Microsoft Corporation

Case Nos. 13-MAG-2814; M9-150



**REPLY MEMORANDUM IN SUPPORT OF MICROSOFT'S MOTION TO VACATE IN
PART AN SCA WARRANT SEEKING CUSTOMER INFORMATION LOCATED
OUTSIDE THE UNITED STATES**

TABLE OF CONTENTS

	Page(s)
I. U.S. Courts Lack The Authority to Issue Extraterritorial Warrants.	2
II. The Instrument at Issue Is an Extraterritorial Warrant, Not a Subpoena or Any Other Form of Compulsory Process The Government Tries to Read Into the SCA.....	3
III. Search Warrants Safeguard Constitutionally Protected Privacy Interests and Are Fundamentally Different From Subpoenas.	7
IV. The Government’s Policy Arguments Fail to Address Important Considerations That Undercut its Position	11
V. Conclusion	13

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Am. Tobacco Co. v. Patterson</i> , 456 U.S. 63 (1982).....	4
<i>Almeida-Sanchez v. United States</i> , 413 U.S. 266 (1973).....	13
<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976).....	8
<i>In re Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW and Information Associated with 12-MJ-8191-DJW Target Email Address</i> , Nos. 12-MJ-8119, 12-MJ-8191, 2012 WL 4383917 (D. Kan. Sept. 21, 2012).....	5
<i>Conn. Nat'l Bank v. Germain</i> , 503 U.S. 249 (1992).....	4, 5
<i>In re Grand Jury Proceedings (Bank of Nova Scotia)</i> , 740 F.2d 817 (11th Cir. 1984)	7
<i>Hubbard v. MySpace, Inc.</i> , 788 F. Supp. 2d 319 (S.D.N.Y. 2011).....	6
<i>In re Marc Rich & Co., A.G.</i> , 707 F.2d 663 (2d Cir. 1983).....	8
<i>Morrison v. Nat'l Australia Bank Ltd.</i> , 130 S. Ct. 2869 (2010).....	7, 8
<i>In re Subpoena Duces Tecum</i> , 228 F.3d 341 (4th Cir. 2000)	9, 10
<i>United States v. Bach</i> , 310 F.3d 1063 (8th Cir. 2002)	5
<i>United States v. Bin Laden</i> , 126 F. Supp. 2d 264 (S.D.N.Y. 2000).....	2
<i>United States v. Calandra</i> , 414 U.S. 338 (1974).....	8
<i>United States v. Davis</i> , 767 F.2d 1025 (2d Cir. 1985).....	12

United States v. Gorshkov,
No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001)3

United States v. Odeh,
552 F.3d 157 (2d Cir. 2008).....2

United States v. Vilar,
No. 05-CR-621, 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007).....2

In re Warrant to Search a Target Computer at Premises Unknown,
No. H-13-234M, 2013 WL 1729765 (S.D. Tex. April 22, 2013).....3, 4

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010)9, 10

United States v. Zovluck,
274 F. Supp. 385 (S.D.N.Y. 1967)8

Statutes

18 U.S.C. § 2703(a)5, 6, 10

18 U.S.C. § 2703(b)(1)(A)10

18 U.S.C. § 2703(b)(1)(B)4, 10

18 U.S.C. § 2703(d)6

18 U.S.C. § 2703(g)6

18 U.S.C. § 2705(a)(1)(B)10

18 U.S.C. § 2705(a)(2).....10

18 U.S.C. § 2709.....6

18 U.S.C. § 2711.....4

50 U.S.C. § 1805.....6

Other Authorities

U.S. Const. amend. IV5

Mutual Legal Assistance Treaty Between the United States and Ireland, T.I.A.S, 1313711

FED. R. CRIM. P. 17(c)(2)8

FED. R. CRIM. P. 413, 5, 6, 7

FED. R. CRIM. P. 41(b)(1)3

RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442 (1987)12

Letter from Mythili Raman, Acting Assistant Attorney General, Criminal Division,
U.S. Department of Justice, to Judge Rcena Raggi, Chair, Advisory Committee on
Criminal Rules (Sept. 18, 20 13), available at
<http://www.uscourts.gov/uscourts/RulesAndPolicies/>7

Email from Christopher B. Harwood, Assistant United States Attorney, United States
Attorney’s Office for the Southern District of New York, to Nathan Wessler,
American Civil Liberties Union (April 19, 2013), *available at*:
<https://www.aclu.org/files/pdfs/email-content-foia/EOUSA%20docs/EOUSA%20response%20email%204.19.13.pdf>.10

United States Attorney Manual (“USAM”) 9:279, available at:
http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00279.htm.12

The Government has served Microsoft with a warrant that seeks, among other things, the contents of a customer's email. Upon inspection, Microsoft determined that the email content data is stored in Ireland and is not located in any form within the United States. There is no dispute that this Court lacks the authority to issue a warrant empowering the Government to execute a search and seizure in Ireland. And yet, the Government insists it should be permitted to compel Microsoft's assistance in doing *indirectly* precisely what it lacks the authority to do *directly* — *i.e.*, conduct a warranted search outside the United States.

The Government seeks to defend its position by arguing that this case does not involve an extraterritorial search and seizure at all. In the Government's view, because the warrant was directed at Microsoft Corporation in the United States, Microsoft is obligated — as it arguably would be if it received a grand jury subpoena — to produce responsive data located anywhere in the world, so long as that data is within Microsoft's possession, custody, or control. In other words, the Government argues that when Congress, in 1986, used the word "warrant" in the Stored Communications Act ("SCA"), it did not mean warrant as that word has been used and understood in criminal law for centuries. Rather, according to the Government, Congress meant to create an entirely new form of warrant (what the Government calls an "SCA Warrant") that functions like a subpoena and therefore can be used to compel an electronic communication service provider to produce data stored outside the United States.

The Government cannot cite a single case in which *any* court has *ever* interpreted the term "warrant" in the SCA to mean "subpoena." This is not surprising. The Government's interpretation ignores both the plain meaning of the SCA and the well-established principle that federal statutes are presumed to lack extraterritorial effect. The Government's interpretation also contravenes long-standing precedent regarding the distinctions between warrants and subpoenas,

ignores the constitutional interests that underlie those distinctions, and upsets the delicate comity analysis that is necessary — and that the Government admits is required — when the United States seeks to compel a private party to produce evidence located abroad.

I. U.S. Courts Lack The Authority to Issue Extraterritorial Warrants.

Microsoft has established, and the Government has not contested, that courts in the United States lack the power to issue warrants authorizing extraterritorial searches and seizures. *See* Memorandum in Support of Microsoft’s Motion to Vacate in Part an SCA Warrant Seeking Customer Information Located Outside the United States (“Br.”) at 5 (citing *United States v. Odeh*, 552 F.3d 157 (2d Cir. 2008) (concluding that U.S. courts are not empowered to issue warrants for foreign searches); *United States v. Vilar*, No. 05-CR-621, 2007 WL 1075041, at *52 (S.D.N.Y. Apr. 4, 2007) (finding no statutory basis for court to issue search warrant to be executed abroad); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 275 (S.D.N.Y. 2000) (same)).

Given the complete absence of authority for extraterritorial warrants, the Government attacks straw man arguments. For instance, rather than addressing the import of the decisions Microsoft cites, the Government recasts them to stand for the wholly irrelevant point that “the Warrant Clause does not limit the Government’s ability to gather evidence overseas.” Government’s Memorandum of Law in Opposition to Microsoft’s Motion to Vacate Email Account Warrant (“Op.”) at 13. Microsoft is not asking the Court to decide whether the Fourth Amendment prohibits the Government from gathering evidence overseas *without a warrant*. The question is whether *the warrant issued in this case* compels Microsoft to assist in an extraterritorial search. The answer must be no. Courts lack the authority to issue extraterritorial warrants, and the SCA only requires Microsoft to comply with a *valid* warrant.

The Government similarly misstates Microsoft's position as being that Rule 41 *forbids* such warrants when issued under the SCA. Op. at 13 ("Microsoft is equally mistaken to suggest that the substantive limitations on conventional search warrants directed to physical premises, as set forth in Rule 41 ... have any impact on SCA warrants"). What Microsoft argues, however, is that "extraterritorial warrants are not *authorized* by Rule 41 or any other source of law." Br. at 5 (emphasis added and capitalization omitted). The Government fails entirely to address this absence of authority — which is confirmed by, *inter alia*, the Supreme Court's express rejection in 1990 of an amendment to Rule 41 that would have authorized extraterritorial search warrants. See Br. at 5.¹

II. The Instrument at Issue Is an Extraterritorial Warrant, Not a Subpoena or Any Other Form of Compulsory Process The Government Tries to Read Into the SCA.

Having little to say about extraterritorial warrants, the Government next argues that the warrant served on Microsoft is *not* extraterritorial because it is "not directed at a physical location" but rather is served on Microsoft Corporation in the United States. Op. at 16. The courts have been clear, however, that a search of electronic data occurs where the data is stored, not at the point(s) from which it may be remotely accessed. See Br. at 7 (citing *United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001); *In re Warrant to Search a Target Computer at Premises Unknown*, No. H-13-234M, 2013 WL

¹ The Government's reliance on the 2001 amendment to the SCA is misplaced. See Op. at 13-14. That amendment authorized the issuance of search warrants by a magistrate judge with jurisdiction over the offense under investigation for electronic data located in a district other than the district of the magistrate judge. The amendment was necessary because such out-of-district warrants would ordinarily be contrary to Rule 41. See FED. R. CRIM. P. 41(b)(1) (authorizing a magistrate judge to "issue a warrant to search for and seize a person or property *located within the district*" (emphasis added)). As we explained in our opening brief, nothing in this amendment empowered magistrate judges to issue out-of-district warrants authorizing the search and seizure of data located outside the United States. See Br. at 9.

1729765 (S.D. Tex. April 22, 2013)). Here, some of the relevant user data is located in Ireland. The warrant therefore purports to authorize a search that would take place in Ireland. *See id.* at 6-8. That should end the analysis. But rather than addressing this point, or the case law Microsoft cites, the Government attempts to rewrite the SCA to avoid the limitations of a warrant altogether.

The Government first suggests that the term “warrant” in the SCA does not actually mean “warrant” but instead means “subpoena.” This ignores the most basic rule of statutory construction. “[C]ourts must presume that a legislature says in a statute what it means and means in a statute what it says there.” *Conn. Nat’l Bank v. Germain*, 503 U.S. 249, 253-54 (1992) (citations and internal quotation marks omitted); *see also Am. Tobacco Co. v. Patterson*, 456 U.S. 63, 68 (1982) (“As in all cases involving statutory construction, our starting point must be the language employed by Congress, and we assume that the legislative purpose is expressed by the ordinary meaning of the words used.” (alteration, citations, and internal quotation marks omitted)).

There is no reason to think Congress actually meant “subpoena” when it used the word “warrant.” The definitional section of the SCA, 18 U.S.C. § 2711, does not assign a meaning to the word “warrant,” much less one that differs from its well-established meaning. And when Congress actually wanted to use the word “subpoena” in the SCA, it had no difficulty doing so. *See, e.g.*, 18 U.S.C. § 2703(b)(1)(B) (authorizing the government to compel the disclosure of information “if the governmental entity ... uses an administrative *subpoena* authorized by Federal or State statute or a Federal or State grand jury or trial *subpoena*.” (emphasis added)).

Faced with the fact that Congress chose the word “warrant” and not “subpoena,” the Government suggests next that when Congress enacted the SCA, it created an entirely novel

form of compulsory process — which the Government terms an “SCA Warrant” — that operates *like* a subpoena and can compel a provider to produce data stored anywhere in the world. The SCA, however, says nothing about “SCA Warrants.” Nor does the statute suggest that Congress meant to vest federal courts with the power to issue “worldwide warrants.” To the contrary, the SCA authorizes the government to compel providers to disclose information “only pursuant to a *warrant* issued using the procedures described in the Federal Rules of Criminal Procedure” 18 U.S.C. § 2703(a) (emphasis added). Congress used the term “warrant,” and it must be assumed that it “says in a statute what it means.” *Conn. Nat’l Bank*, 503 U.S. at 254. As the Eighth Circuit observed in *United States v. Bach*, “[w]hile warrants for electronic data are often served like subpoenas (via fax), Congress called them warrants and we find that Congress intended them to be treated as warrants.” 310 F.3d 1063, 1066 n.1 (8th Cir. 2002).²

In fact, the SCA does not in any way *create* authority for courts to issue warrants. Section 2703(a) merely authorizes the government to compel providers to produce information if served with a warrant — in other words, to provide assistance to the Government in executing the underlying warrant. The statute thus incorporates by reference an existing form of compulsory process derived from other established sources of law, including the Fourth Amendment and Fed. R. Crim. P. 41. See *In re Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW and Information Associated with 12-MJ-8191-DJW Target Email Address*, Nos. 12-MJ-8119, 12-MJ-8191, 2012 WL 4383917, *5 (D. Kan. Sept. 21, 2012) (“A warrant seeking stored electronic communications such as emails or faxes therefore should be subject to

² The Government criticizes the court’s decision in *Bach* for not “elaborat[ing] on its reasoning or the implications of its observations,” and asserts that the quoted language was an “academic point” made in a footnote. Op. at 17-18 & n.11. But the Government fails to identify any flaw in the *Bach* court’s common-sense conclusion that Congress intended “warrants” issued under the SCA to be treated like warrants and not like subpoenas. See *id.*

the same basic requirements of any search warrant”). Where Congress has sought to create new forms of compulsory process, both in the SCA and in other statutes, it has done so clearly. *See, e.g.*, 18 U.S.C. § 2703(d) (authorizing disclosure orders based on “specific and articulable facts showing that there are reasonable grounds to believe that the [information is] relevant and material to an ongoing criminal investigation”); 18 U.S.C. § 2709 (authorizing “National Security Letters” to compel production of certain non-content information); 50 U.S.C. § 1805 (authorizing surveillance orders under the Foreign Intelligence Surveillance Act based on probable cause). Here, however, Congress decided not to create a new form of process but opted instead to rely on the pre-existing warrant authority.

Nor does the fact that the SCA abrogates specific aspects of Rule 41 support the Government’s interpretation. The Government notes that (i) the SCA requires that warrants comply only with the “procedures described in” Rule 41 (*i.e.*, not its substantive provisions), and (ii) the statute eliminates the traditional requirement of an officer’s presence when a warrant is executed. *See* Op. at 14 (citing 18 U.S.C. § 2703(a), (g); *Hubbard v. MySpace, Inc.*, 788 F. Supp. 2d 319, 325 n.18 (S.D.N.Y. 2011)). This does not imply that Congress intended to create a new type of “worldwide warrant.” If anything, it shows the opposite. Specifically, Congress chose to draft the SCA to include narrowly tailored changes to pre-existing warrant procedures, but at the same time declined to alter the well-established principle that courts lack authority to issue extraterritorial warrants.

In arguing to the contrary, the Government runs squarely into the presumption against extraterritoriality. The Government claims that “neither the text nor the structure of the SCA *limits* the scope of compelled disclosure . . . to records maintained within the United States.” Op. at 6 (capitalization omitted and emphasis added). This approach to statutory interpretation is

upside down. The Supreme Court has explained unequivocally that “[w]hen a statute gives no clear indication of an extraterritorial application, it has none.” *Morrison v. Nat’l Australia Bank Ltd.*, 130 S. Ct. 2869, 2878 (2010). The SCA contains no indication, let alone a *clear* indication, that Congress intended warrants issued under the statute to authorize the search and seizure of data located outside the United States — a proposition with which the Government has expressly agreed in proposing amendments to Rule 41. See Letter from Mythili Raman, Acting Assistant Attorney General, Criminal Division, U.S. Department of Justice, to Judge Reena Raggi, Chair, Advisory Committee on Criminal Rules (Sept. 18, 2013) (the “Raman Letter”) (“In light of the presumption against international extraterritorial application ... this [proposed] amendment [to Rule 41] does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries.”).³

III. Search Warrants Safeguard Constitutionally Protected Privacy Interests and Are Fundamentally Different From Subpoenas.

The Government strains to interpret “warrant” in the SCA to mean “subpoena” so as to take advantage of a line of cases often referred to as the *Bank of Nova Scotia* (or “BNS”) doctrine. These cases hold that a party subject to U.S. jurisdiction can be compelled by grand jury subpoena to produce evidence stored outside the United States so long as the evidence is within the party’s “possession, custody, or control.” See Op. at 9 (citing, *inter alia*, *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984)).⁴ While the

³ The Government soft-pedals the Raman Letter by excerpting several inapposite passages, see Op. at 15-16, but it tellingly has nothing to say about the letter’s key acknowledgement (quoted above) that the SCA does not authorize courts to issue warrants for extraterritorial searches and seizures.

⁴ Microsoft does not concede that the BNS doctrine is good law after the Supreme Court’s reinvigoration of the presumption against extraterritoriality in *Morrison v. National Australia Bank Ltd.*, 130 S. Ct. 2869, 2878 (2010). The Court need not address this issue because even if (continued...)

Government cites several cases for the basic *BNS* principle, it fails to identify *any* in which a court has applied *BNS* in the context of a search warrant. We are aware of none.

The Government's inability to support its argument with actual precedent is not a coincidence. Warrants and grand jury subpoenas are fundamentally different types of legal process. The grand jury is vested with "wide latitude to inquire into violations of criminal law," *United States v. Calandra*, 414 U.S. 338, 343 (1974), and when it issues a subpoena, the recipient is compelled as a matter of "public duty" to collect and produce the responsive evidence. *In re Marc Rich & Co., A.G.*, 707 F.2d 663, 670 (2d Cir. 1983). And notably, the recipient of a grand jury subpoena may move the court *ex ante* to modify or quash the subpoena. *See* FED. R. CRIM. P. 17(c)(2).

A warrant, in contrast, is a constitutionally limited, *ex parte* authorization from a court that permits the Government to trespass upon private property. Unlike a subpoena-recipient, the target of a warranted search is neither able to contest the search *ex ante* nor "required to aid in the discovery, production, or authentication of incriminating evidence." *Andresen v. Maryland*, 427 U.S. 463, 473-74 (1976). Moreover, "[t]he authority to search [granted by a warrant] is limited to the place described in the warrant and does not include additional or different places." *United States v. Zovluch*, 274 F. Supp. 385, 390 (S.D.N.Y. 1967). Warrants thus authorize a narrow yet fundamentally more intrusive exercise of government power than the self-directed process called for by a subpoena. As noted by the Fourth Circuit, "the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant demand the safeguard of demonstrating probable cause to a neutral judicial officer before the warrant issues, whereas the

the *BNS* doctrine survives *Morrison*, it does not apply to warrants for the reasons discussed herein.

issuance of a subpoena initiates an adversary process that can command the production of documents and things only after judicial process is afforded.” *In re Subpoena Duces Tecum*, 228 F.3d 341, 348 (4th Cir. 2000).

Despite the historical and fundamental differences between the two forms of process, the Government takes the extraordinary position that Microsoft has engaged in a “muddled reading” of the SCA by simply giving effect to the plain meaning of the word “warrant.” The Government argues that this reading would be contrary to the statute’s “upside-down pyramid” structure insofar as law enforcement could conceivably compel the disclosure of more information with a subpoena than with a warrant. *See* Op. at 7-8 (“It cannot be that Congress intended that a subpoena can properly require a service provider to produce emails regardless of where they are stored, but a 2703(d) Order or SCA Warrant — issued pursuant to higher standards and court approval — imposes more limited obligations on a U.S. service provider.”). But given that the subpoena power is exercised on notice to the customer or subscriber whose data is sought by the subpoena, and may sweep more broadly than the warrant authority, the claimed “absurdity” identified by the Government is illusory. The Government’s argument fails for two reasons.

First, the SCA “upside-down pyramid” that the Government portrays is, in practice, no pyramid at all — at least not since 2010, when the Sixth Circuit held that the Fourth Amendment requires the Government to obtain a warrant to search for and seize email content. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). We understand that the Government’s practice since *Warshak* has been to obtain a warrant when seeking access to email contents in

criminal cases.⁵ Given that the Government appears only to use the warrant section of the SCA when seeking the contents of stored electronic communications, its structural argument rings hollow.

Second, and more fundamentally, the Government's argument ignores the SCA's use of different notice provisions for the different forms of process. If the Government serves a warrant under the SCA, it is not required to notify the customer, *see* 18 U.S.C. § 2703(a), (b)(1)(A) — a practice that is consistent with established precedent applicable to physical searches and seizures. *See In re Subpoena Duces Tecum*, 228 F.3d at 348 (“A warrant is a judicial authorization to a law enforcement officer to search or seize persons or things. To preserve advantages of speed and surprise, the order is issued *without prior notice* and is executed, often by force, with an unannounced and unanticipated physical intrusion” (emphasis added)).

In contrast, the subpoena power under the SCA is generally exercised *on notice* to the customer or subscriber whose data is sought, and may therefore have a wider reach than the warrant authority. *See* 18 U.S.C. § 2703(b)(1)(B).⁶ The SCA's notice requirement for subpoenas permits the customer to vindicate his or her privacy (or other) interests by moving to quash the subpoena. *See In re Subpoena Duces Tecum*, 228 F.3d at 348 (“A subpoena, on the

⁵ *See* Email from Christopher B. Harwood, Assistant United States Attorney, United States Attorney's Office for the Southern District of New York, to Nathan Wessler, American Civil Liberties Union (April 19, 2013) (confirming that the United States Attorney's Office for the Southern District of New York has not, since *Warshak*, “authorized a request to a court for access to the contents of a person's private electronic communications for law enforcement purposes without a warrant or on a standard less than probable cause”), *available at*: <https://www.aclu.org/files/pdfs/email-content-foia/EOUSA%20docs/EOUSA%20response%20email%204.19.13.pdf>.

⁶ The SCA allows the Government to delay notice to the target of a subpoena for ninety days “upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result[.]” 18 U.S.C. § 2705(a)(1)(B), with the term “adverse result” defined with particularity in the statute. *See id.* § 2705(a)(2).

other hand [*i.e.*, unlike a warrant], commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands As judicial process is afforded before any intrusion occurs, the proposed intrusion is regulated by, *and its justification derives from*, that process.” (emphasis added)).

In short, subpoenas have a wider reach than warrants, but the statute provides an opportunity to challenge them *ex ante*. Warrants, while more intrusive than subpoenas, are at the same time more limited; they are constrained both by the Fourth Amendment’s requirements of probable cause and particularity, and by the inherent inability of federal courts to authorize searches and seizures outside the United States. This trade-off, embedded in the structure of the SCA, makes eminent sense. The Government’s muddling of the distinction between the two forms of process makes no sense.

IV. The Government’s Policy Arguments Fail to Address Important Considerations That Undercut its Position.

The Government argues that Microsoft’s motion should be denied as a matter of policy because it would “severely undercut criminal investigations.” *Op.* at 19. It bases its argument on the mistaken notion that “Microsoft appears to believe that the mere fact that records are stored abroad renders them beyond the scope of compulsory process.” *Id.* Microsoft did not say this. Indeed, the Government could compel it to disclose email content stored in Dublin by proceeding under the Ireland-United States Mutual Legal Assistance Treaty (“MLAT”), which entered into force on August 11, 2009. *See* Mutual Legal Assistance Treaty Between the United States and Ireland, T.I.A.S. 13137. The Government shrugs off this alternative by complaining that “Mutual Legal Assistance Treaties and letters rogatory are slow and cumbersome processes.” *Op.* at 21. But even if this is true (and the Government offers no evidence it is), inconvenience cannot justify a blatant disregard of the SCA’s plain language.

Considerations of international comity further undercut the Government's policy arguments. The Second Circuit has explicitly recognized that the law of foreign jurisdictions may forbid compliance with subpoenas that seek data stored within their borders, and has held that international comity may justify limitations on the Government's subpoena power. *See United States v. Davis*, 767 F.2d 1025, 1033-34 (2d Cir. 1985) (adopting a multi-factor analysis set out in the Restatement of Foreign Relations Law "in evaluating the propriety of a subpoena directing the production of information or documents located abroad when such production would violate the law of the state in which the documents are located"); *see also* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442 (1987).

The Government itself recognizes that *Bank of Nova Scotia* subpoenas can threaten international relations. According to the United States Attorneys' Manual, "foreign governments strongly object to [*BNS*] subpoenas, contending that they constitute an improper exercise of United States jurisdiction." United States Attorney Manual ("USAM") 9:279, available at: http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00279.htm.⁷

⁷ In deciding whether to approve a *BNS* subpoena, the USAM requires federal prosecutors to weigh the following considerations:

- 1) The availability of alternative methods for obtaining the records in a timely manner, such as use of mutual assistance treaties, tax treaties or letters rogatory;
- 2) The indispensability of the records to the success of the investigation or prosecution; and
- 3) The need to protect against the destruction of records located abroad and to protect the United States' ability to prosecute for contempt or obstruction of justice for such destruction.

Id.

Where a subpoena calls for data stored outside the United States, a motion to quash provides an orderly mechanism for courts to conduct a *Davis* multi-factor comity analysis before requiring the production of data in violation of foreign law. Warrant procedures do not provide this mechanism. In fact, the Government and courts may not always know whether a warrant calls for the production of data stored outside the United States, which would make it impossible for either the Government or the court issuing the warrant to consider the comity principles articulated in *Davis* and the USAM. These troubling consequences are avoided if warrants directed at electronic communications service providers for communications data covered by the SCA are interpreted under traditional principles of territoriality, as the plain language of the statute requires.

In short, the Government's policy concerns do not change the text of the SCA, nor should they create authority for extraterritorial warrants where none exists. Microsoft freely concedes that the plain meaning of the SCA may constrain the Government's exercise of investigative powers. That is nothing new in our constitutional system. As the Supreme Court observed in *Almeida-Sanchez v. United States*, "[t]he needs of law enforcement stand in constant tension with the Constitution's protections of the individual against certain exercises of official power. It is precisely the predictability of these pressures that counsels a resolute loyalty to constitutional safeguards." 413 U.S. 266, 273 (1973).


V. Conclusion

For the foregoing reasons and those set forth in its opening brief, Microsoft respectfully requests that the Court vacate that part of the warrant calling for the search and seizure of customer information located outside the United States.


Dated: March 14, 2014

Respectfully submitted,

MICROSOFT CORPORATION



Guy Petrillo
Nelson A. Boxer
PETRILLO KLEIN & BOXER LLP
655 Third Avenue
New York, NY 10017
Tel: 212.370.0330
gpetrillo@pkblp.com
nboxer@pkblp.com



Nancy Kestenbaum SDNY Bar # NK9768
Claire Catalano SDNY Bar # CC7432
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
Tel: 212-841-1000
Fax: 212-841-1010
nkestenbaum@cov.com
ccatalano@cov.com

James M. Garland*
Alexander A. Berengaut*
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401
Tel: 202.662.6000
Fax: 202.662.6291
jgarland@cov.com
aberengaut@cov.com

**Admitted pro hac vice*

Counsel for Microsoft Corporation

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Search of The PREMISES
known and described as the email account
[REDACTED]@MSN.COM, which is
controlled by Microsoft Corporation

Case Nos. 13-MAG-2814; M9-150

CERTIFICATE OF SERVICE

I, Claire Catalano, hereby certify that on the 14th Day of March, 2014, I caused a true and correct copy of the REPLY MEMORANDUM IN SUPPORT OF MICROSOFT'S MOTION TO VACATE IN PART AN SCA WARRANT SEEKING CUSTOMER INFORMATION LOCATED OUTSIDE THE UNITED STATES to be served via hand delivery upon the United States Attorney for the Southern District of New York at the following address:

ATTN: Andrea Surratt
United States Attorney for the Southern District of New York
One St. Andrews Plaza
New York City, NY 10007



Claire Catalano SDNY Bar # CC7432
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
Tel: 212-841-1000
Fax: 212-841-1010
ccatalano@cov.com